REMARKS

Applicants appreciate the continued thorough examination of the present application that is evidenced in the Final Official Action of February 13, 2006 (the "Final Action"). Applicants request entry of the amendments to Claims 1, 9, 25 and 26 as provided in the Listing of Claims. Claims 7-8 and 24 have been cancelled. In particular, Claim 1 has been amended to include the recitations of cancelled Claims 7 and 8. Claims 25 and 26 have been amended to include similar recitations as in cancelled Claims 7 and 8. Claim 9 has been amended to correct the claim dependency following cancellation of Claim 7. Claims 18-20 have been amended to clarify certain claim language. For the reasons discussed below, Applicants respectfully request reconsideration of the present application and submit that the claims, as amended, are allowable over the art of record.

Status of the Claims

Claims 1-26 are pending in the present application. Claims 1, 21, and 24-26 stand rejected under 35 U.S.C. § 102(b) as anticipated by U.S. Patent No. 6,070,198 to Krause et al. ("Krause"). Claims 2-17, 19, and 22-23 stand rejected under 35 U.S.C. § 103(a) as unpatentable over Krause in view of Mod_SSL manual. Claim 18 stands rejected as unpatentable under 35 U.S.C. § 103(a) over Krause in view of U.S. Patent No. 5,974,549 to Golan. Claim 20 stands rejected as unpatentable under 35 U.S.C. § 103(a) over Krause in view of Golan and further in view of U.S. Patent No. 6,801,927 to Smith et al. ("Smith").

The Independent Claims Are Patentable Over the Cited References

Claim 1 has been amended to include the recitations of cancelled Claims 7 and 8, which were rejected as unpatentable over Krause in view of Mod_SSL manual. Applicants submit that Claim 1, as amended, is patentable over Krause in view of Mod_SSL manual. In particular, Claim 1, as amended, recites (emphasis added):

> 1. (Currently Amended) A method of improving security processing in a computing network, comprising:
>
> providing security processing in an operating system kernel;

providing an application program which makes use of the operating system kernel during execution;

executing the application program;

selectably securing at least one communication of the executing application program with a remotely executing application program using the provided security processing in the operating system kernel;

providing, in the secure processing, support for at least one security directive; and

invoking, during execution of the provided application program, the at least one security directive.

According to some embodiments of the invention, an application that has some SSL awareness may utilize kernel-based security processing functionality to obtain desired information about a communication. As explained in the Specification, "[p]referably, one or more API calls for requesting client information are supported by an implementation of the present invention. The application may then issue an API call such as 'GET_CLIENT_CERT' or 'GET_CLIENT_ID.' The stack responds accordingly, providing the requested information. The API calls are referred to equivalently herein as 'SSL directives.'" *See*, Specification, page 14, ll. 7-11. Thus, by performing a method as recited in Claim 1, only a minimal amount of security processing (that is, invoking the API and receiving its response) may be added to the application. *See*, Specification, page 7, ll. 16-18.

The Final Action notes that Krause does not expressly disclose providing support for at least one security directive, but states that Mod_SSL discloses different classes of directives that can be used as security directives. Final Action at 14. While Mod_SSL discusses certain directives that may be invoked to perform security processing, it is important to note that Claim 1 is not simply directed to a method of providing and invoking security directives. Rather, Claim 1, as amended, is directed to a method of providing security processing in an ***operating system kernel*** that ***also*** supports at least one security directive that may be invoked by an executing application program. Such functionality is not taught or suggested by Krause or Mod_SSL, alone or in combination.

In contrast, as noted in the Final Action, the system of Krause performs security processing for application programs without providing support for security directives that may be

invoked by the executing application programs. Thus, Applicants respectfully submit that Claim 1, as amended, is patentable over the cited references.

Similar recitations as added to Claim 1 have been added to Claims 25-26. Accordingly, Applicants submit that Claims 25-26 are patentable for at least these reasons.

The Dependent Claims Are Patentable Over the Cited References

The dependent claims are patentable at least as per the patentability of Claim 1. In addition, many of the dependent claims are separately patentable. For example, Claim 12 recites providing, in the secure processing, support for a security directive that requests selectably securing the at least one communication of the executing application program to begin operating. Similarly, Claim 13 recites providing, in the secure processing, support for a security directive that requests selectably securing the at least one communication of the executing application program to stop operating. As noted above, the system of Krause performs security processing for application programs without providing support for security directives that may be invoked by the executing application programs. In contrast, in a system configured to perform a method according to Claims 12 and/or 13, an application having SSL awareness may control some aspects of security processing, such as starting and/or stopping the security processing. *See*, Specification, p. 16, ll. 17-19. Thus, Claims 12 and 13 are patentable for at least these additional reasons.

With respect to Claims 18-19, the Final Action states that Krause discloses a method in which the application program comprises calls that invoke the security processing and the corresponding security functions. As examples, the Final Action refers to calls such as copyin() and send() functions described in Krause. In contrast, Claims 18 and 19 have been amended to clarify that the calls made by the application program that that invoke security processing are security directives. As noted above, the system of Krause performs security processing for application programs without providing support for security directives that may be invoked by the executing application programs. In contrast, a system configured to perform a method according to Claims 18 and/or 19 may accommodate client and/or server applications that are

SSL-aware and are coded to use security directives for invoking SSL APIs. *See*, Specification, p. 22, ll. 14-16. Thus, Claims 18 and 19 are patentable for at least these additional reasons.

CONCLUSION

In light of the above amendments and remarks, Applicants respectfully submit that the above-entitled application is now in condition for allowance. Favorable reconsideration of this application, as amended, is respectfully requested. If, in the opinion of the Examiner, a telephonic conference would expedite the examination of this matter, the Examiner is invited to call the undersigned attorney at (919) 854-1400.

Respectfully submitted,

David C. Hall
Registration No. 38,904
Attorney for Applicants

Customer Number 46589
Myers Bigel Sibley & Sajovec, P.A.
P.O. Box 37428
Raleigh, NC 27627
919-854-1400
919-854-1401 (Fax)